Recon-Web: Comprehensive Reconnaissance Guide

Introduction

What is Recon-web?

Recon-web is the web interface for Recon-ng, providing a user-friendly GUI to interact with the Recon-ng framework through a browser.

What is Recon-ng?

Recon-ng is a full-featured reconnaissance framework written in Python. It provides a powerful environment for conducting open-source web-based reconnaissance quickly and thoroughly.

Why Use These Tools?

- **Automated OSINT**: Gather intelligence from public sources automatically
- **Modular Design**: Use only the modules you need
- **Data Management**: Organize findings in a structured database
- **Professional Reporting**: Generate comprehensive reports for penetration testing

Prerequisites

System Requirements

- Kali Linux (running on Oracle VirtualBox)
- Python 3.6 or higher
- Internet connection
- At least 2GB RAM allocated to VM
- 20GB free disk space

Required Knowledge

- Basic Linux command line
- Understanding of networking concepts

- Familiarity with OSINT techniques
- Basic cybersecurity principles

Installation

Step 1: Update Kali Linux

bash

sudo apt update && sudo apt upgrade -y

Step 4: Install Recon-web (Optional)

bash

cd /opt

sudo git clone https://github.com/lanmaster53/recon-web.git

cd recon-web

sudo pip3 install -r requirements.txt

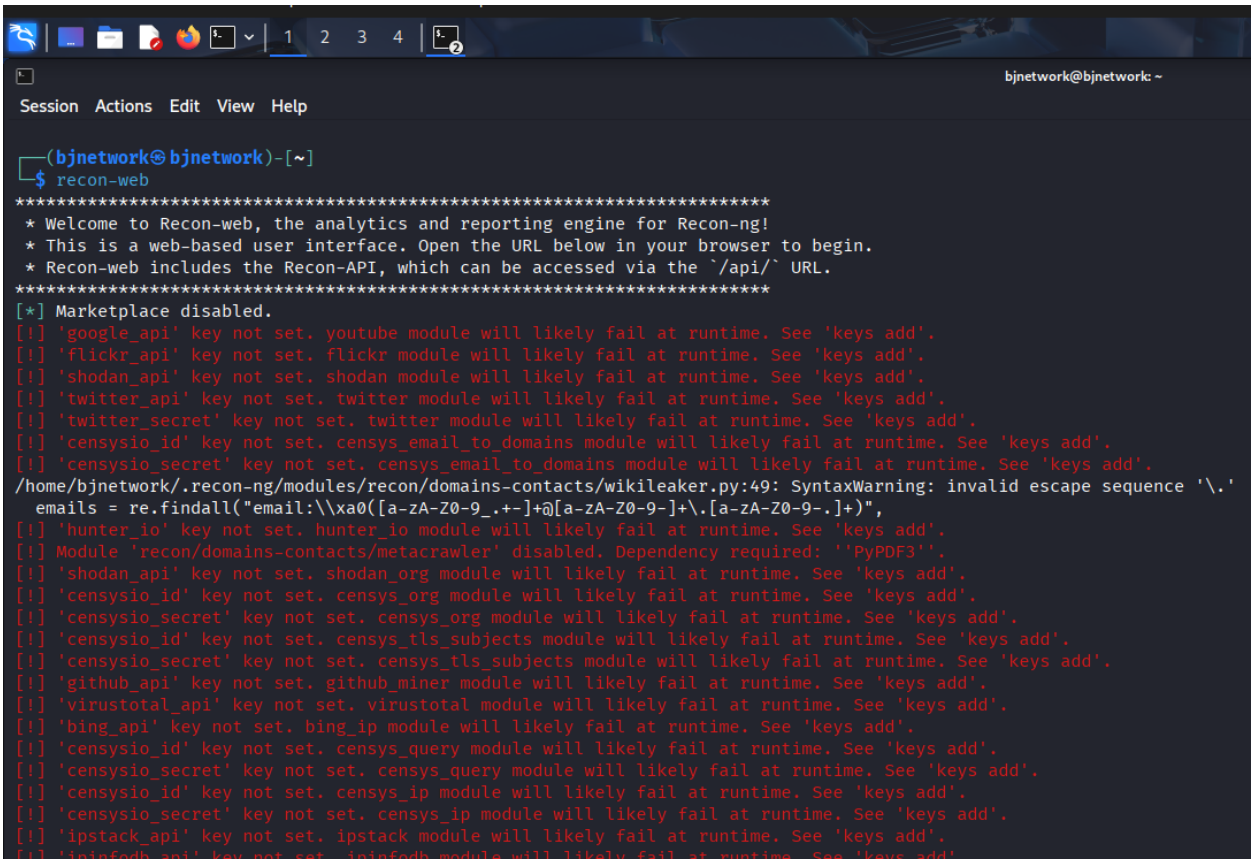
Recon-web Overview

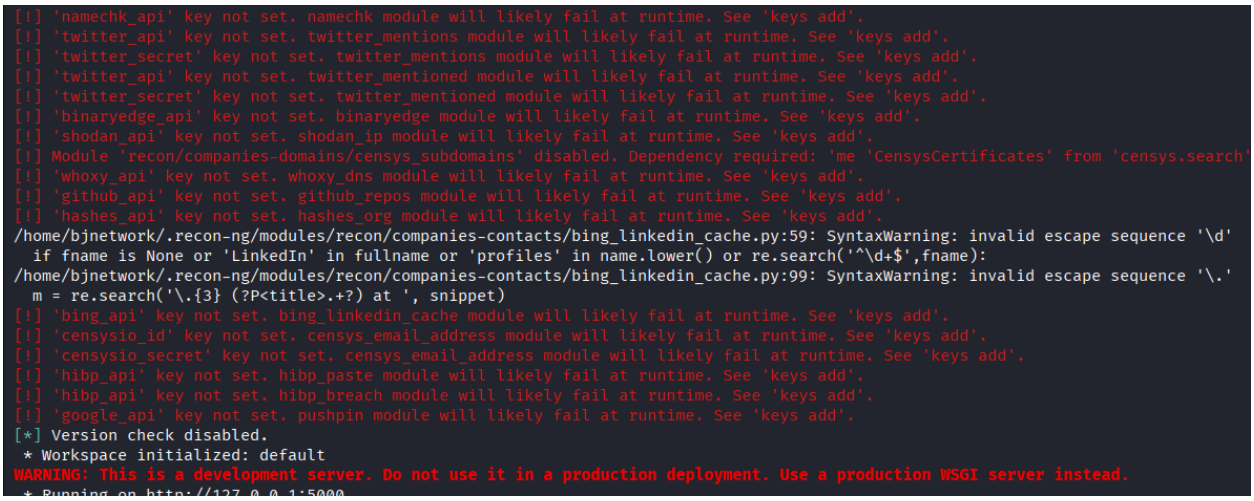
Starting Recon-web

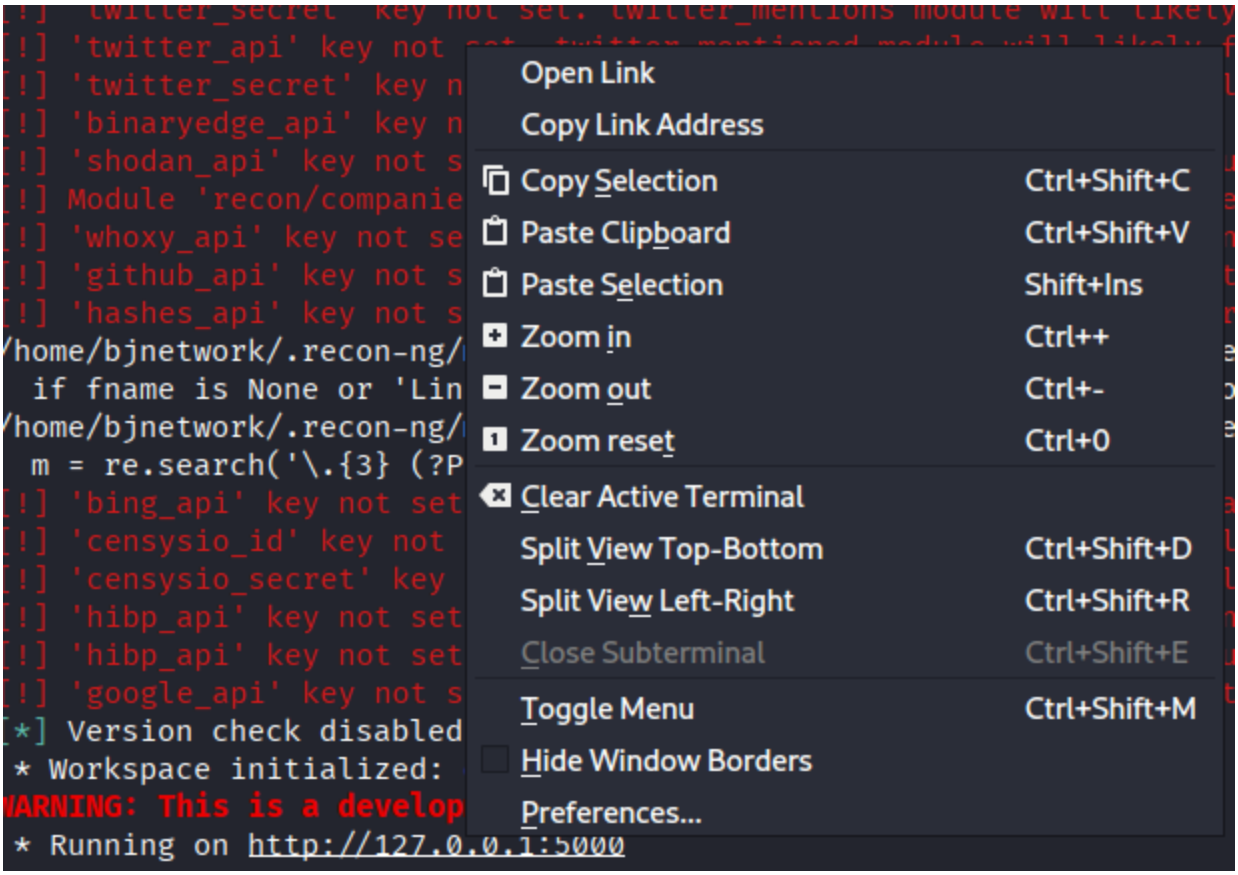
bash

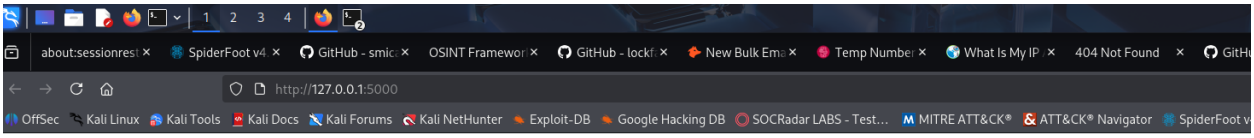
cd /opt/recon-web

python3 recon-web.py


1 2 3 4
bjnetwork@bjnetwork: ~
Session Actions Edit View Help
(bjnetwork㉿bjnetwork)-[~]
$ recon-web
* Welcome to Recon-web, the analytics and reporting engine for Recon-ng!
* This is a web-based user interface. Open the URL below in your browser to begin.
* Recon-web includes the Recon-API, which can be accessed via the `/api/` URL.
[*] Marketplace disabled.
[!] 'google_api' key not set. youtube module will likely fail at runtime. See 'keys add'.
[!] 'flickr_api' key not set. flickr module will likely fail at runtime. See 'keys add'.
[!] 'shodan_api' key not set. shodan module will likely fail at runtime. See 'keys add'.
[!] 'twitter_api' key not set. twitter module will likely fail at runtime. See 'keys add'.
[!] 'twitter_secret' key not set. twitter module will likely fail at runtime. See 'keys add'.
[!] 'censysio_id' key not set. censys_email_to_domains module will likely fail at runtime. See 'keys add'.
[!] 'censysio_secret' key not set. censys_email_to_domains module will likely fail at runtime. See 'keys add'.
/home/bjnetwork/.recon-ng/modules/recon/domains-contacts/wikileaker.py:49: SyntaxWarning: invalid escape sequence '\.'
emails = re.findall("email:\\xa0([a-zA-Z0-9_.+-]+@[a-zA-Z0-9-]+\.[a-zA-Z0-9-.]+)",
[!] 'hunter_io' key not set. hunter_io module will likely fail at runtime. See 'keys add'.
[!] Module 'recon/domains-contacts/metacrawler' disabled. Dependency required: ''PyPDF3''.
[!] 'shodan_api' key not set. shodan_org module will likely fail at runtime. See 'keys add'.
[!] 'censysio_id' key not set. censys_org module will likely fail at runtime. See 'keys add'.
[!] 'censysio_secret' key not set. censys_org module will likely fail at runtime. See 'keys add'.
[!] 'censysio_id' key not set. censys_tls_subjects module will likely fail at runtime. See 'keys add'.
[!] 'censysio_secret' key not set. censys_tls_subjects module will likely fail at runtime. See 'keys add'.
[!] 'github_api' key not set. github_miner module will likely fail at runtime. See 'keys add'.
[!] 'virustotal_api' key not set. virustotal module will likely fail at runtime. See 'keys add'.
[!] 'bing_api' key not set. bing_ip module will likely fail at runtime. See 'keys add'.
[!] 'censysio_id' key not set. censys_query module will likely fail at runtime. See 'keys add'.
[!] 'censysio_secret' key not set. censys_query module will likely fail at runtime. See 'keys add'.
[!] 'censysio_id' key not set. censys_ip module will likely fail at runtime. See 'keys add'.
[!] 'censysio_secret' key not set. censys_ip module will likely fail at runtime. See 'keys add'.
[!] 'ipstack_api' key not set. ipstack module will likely fail at runtime. See 'keys add'.


[!] 'namechk_api' key not set. namechk module will likely fail at runtime. See 'keys add'.
[!] 'twitter_api' key not set. twitter_mentions module will likely fail at runtime. See 'keys add'.
[!] 'twitter_secret' key not set. twitter_mentions module will likely fail at runtime. See 'keys add'.
[!] 'twitter_api' key not set. twitter_mentioned module will likely fail at runtime. See 'keys add'.
[!] 'twitter_secret' key not set. twitter_mentioned module will likely fail at runtime. See 'keys add'.
[!] 'binaryedge_api' key not set. binaryedge module will likely fail at runtime. See 'keys add'.
[!] 'shodan_api' key not set. shodan_ip module will likely fail at runtime. See 'keys add'.
[!] Module 'recon/companies-domains/censys_subdomains' disabled. Dependency required: 'me 'CensysCertificates' from 'censys.search'
[!] 'whoxy_api' key not set. whoxy_dns module will likely fail at runtime. See 'keys add'.
[!] 'github_api' key not set. github_repos module will likely fail at runtime. See 'keys add'.
[!] 'hashes_api' key not set. hashes_org module will likely fail at runtime. See 'keys add'.
/home/bjnetwork/.recon-ng/modules/recon/companies-contacts/bing_linkedin_cache.py:59: SyntaxWarning: invalid escape sequence '\d'
if fname is None or 'LinkedIn' in fullname or 'profiles' in name.lower() or re.search('^\d+$',fname):
/home/bjnetwork/.recon-ng/modules/recon/companies-contacts/bing_linkedin_cache.py:99: SyntaxWarning: invalid escape sequence '\.'
m = re.search('\.{3} (?P<title>.+?) at ', snippet)
[!] 'bing_api' key not set. bing_linkedin_cache module will likely fail at runtime. See 'keys add'.
[!] 'censysio_id' key not set. censys_email_address module will likely fail at runtime. See 'keys add'.
[!] 'censysio_secret' key not set. censys_email_address module will likely fail at runtime. See 'keys add'.
[!] 'hibp_api' key not set. hibp_paste module will likely fail at runtime. See 'keys add'.
[!] 'hibp_api' key not set. hibp_breach module will likely fail at runtime. See 'keys add'.
[!] 'google_api' key not set. pushpin module will likely fail at runtime. See 'keys add'.
[*] Version check disabled.
* Workspace initialized: default
WARNING: This is a development server. Do not use it in a production deployment. Use a production WSGI server instead.





[recon-ng] [default]

pushpin xlsx

Tables: companies contacts credentials domains hosts leaks locations netblocks ports profiles pushpins repositories vulnerabilities

module activity

hosts
2
domains
0
companies
0
netblocks
0
locations
0

recon/domains-hosts/hackertarget
3
recon/credentials-credentials/bozocrack
1

Features

- Visual workspace management
- Module execution through GUI
- Real-time results display
- Report generation interface

Information Analysis

Critical Information to Look For

During Scanning

1. **Subdomains**: Identify attack surface expansion
2. **Email Addresses**: Potential phishing targets or social engineering vectors
3. **Employee Names**: Social engineering reconnaissance
4. **IP Addresses**: Network infrastructure mapping
5. **Technologies Used**: Identify potential vulnerabilities
6. **DNS Records**: Understand network configuration
7. **Exposed Services**: Find potential entry points

After Scanning

1. **Pattern Recognition**: Look for naming conventions
2. **Infrastructure Analysis**: Cloud vs on-premise hosting
3. **Third-party Services**: Identify external dependencies
4. **Data Leaks**: Exposed credentials or sensitive information
5. **Attack Surface**: Entry points for penetration testing

How to Use This Information

For Security Professionals

- **Penetration Testing**: Identify targets for authorized testing

- **Vulnerability Assessment**: Discover exposed services
- **Security Auditing**: Evaluate organizational exposure
- **Incident Response**: Map infrastructure during investigations

For Red Team Operations

- **Social Engineering**: Build targeted phishing campaigns
- **Infrastructure Mapping**: Understand network topology
- **Vulnerability Exploitation**: Identify weak points
- **Persistence Planning**: Find stable infrastructure points

For Blue Team Defense

- **Asset Discovery**: Know what you're protecting
- **Exposure Reduction**: Remove unnecessary public information
- **Monitoring**: Set up alerts for exposed services
- **Security Posture**: Understand external visibility

Advantages & Disadvantages

Advantages

1. **Modular Architecture**
    - Use only needed modules
    - Easy to extend functionality
    - Community-driven development
2. **Database Integration**
    - Organized data storage
    - Relational data management
    - Easy data querying and export
3. **Automation**
    - Reduce manual OSINT work
    - Consistent methodology
    - Time-efficient reconnaissance

4. **Professional Output**
    - Multiple report formats
    - Structured data presentation
    - Easy to share findings
5. **Active Development**
    - Regular updates
    - Growing module marketplace
    - Community support

Disadvantages

1. **API Key Dependency**
    - Many modules require API keys
    - Rate limiting on free APIs
    - Cost for premium services
2. **Learning Curve**
    - Command-line interface complexity
    - Module understanding required
    - Database knowledge helpful
3. **Legal Considerations**
    - Must have authorization
    - Potential for misuse
    - Ethical boundaries required
4. **Data Accuracy**
    - Depends on source reliability
    - May contain outdated information
    - False positives possible
5. **Detection Risk**
    - Activities may be logged

- IP address exposure
- Rate limiting triggers

Security Best Practices

Legal & Ethical Guidelines

1. **Authorization First**
    - Always obtain written permission
    - Stay within scope boundaries
    - Document all activities
2. **Responsible Disclosure**
    - Report findings to proper channels
    - Allow time for remediation
    - Don't publicly disclose vulnerabilities prematurely

Conclusion

Recon-ng and Recon-web are powerful reconnaissance tools that, when used ethically and legally, provide invaluable intelligence for security professionals. Always prioritize authorization, responsible disclosure, and operational security in your reconnaissance activities.

Remember: With great power comes great responsibility. Use these tools only for authorized security testing and research.